경영유의사항 · 개선사항 공개안

Ⅰ. 금융회사명 : 악사손해보험주식회사

Ⅱ. 조치일 : 2022. 2. 28.

Ⅲ. 조치내용

대 상	내 용
기 관	개선사항 5건

Ⅳ. 조치대상사실

1. 개선사항

가. 재해복구훈련 범위 및 절차 불합리

회사는 「전자금융감독규정」 제23조(비상대책 등의 수립·운용)에 따라 IT서비스연속성 계획(IT Service Continuity Plan)을 마련하고 주요 업무가 중단되는 상황에서 신속히 업무의 본래 상태 혹은 조직이 허용 가능한 수준으로 복구될 수 있도록 매년 재해복구 훈련을 실시하고 있으나

대고객 업무에 해당하는 인터넷 홈페이지, 모바일앱 관련 시스템을 핵심업무에 포함하지 아니하여 재해복구시스템 구축 및 훈련이 이루어지지 않아 재해발생 등 비상상황이 발생할 경우 대고객 서비스 업무를 원활하게 제공하지 못할 우려가 있고

재해복구훈련에 현업 부서가 참여하지 않아* 훈련시 복구된 시스템 및 데이터에 대해 현업 부서 직원이 검증하지 않았고, 재해복구훈련 결과보고서에 훈련결과 성공 여부 및 수행시간만 기술하고 상세 검증 결과**를 포함하지 않고 있어 실질적인 재해복구훈련이 이루어지지 않을 우려가 있으므로

* '17년도까지는 현업 부서가 참여하였으나 '18~'20년도에 미참여

** 점검 대상 시스템, 점검자, 점검 시간, 입력조건, 조회조건, 검증 결과 등

재해발생 시 대고객 서비스를 원활하게 제공하고 재해복구훈련의 실효성을 확보하기 위하여 핵심업무 범위 확대, 현업부서 직원 훈련 참여 및 검증결과 기록 상세화 등 관련 절차를 개선하시기 바람

나. 전자금융기반시설 취약점 분석·평가 미흡

회사는 「전자금융감독규정」 제37조의2에 따라 전자금융기반시설(연 1회) 및 홈페이지(반기별 1회)에 대해 외부기관(□□)에 위탁하여 주기적으로 취약점 분석·평가를 수행하고 있으나

2020년도 및 2021년도 전자금융기반시설 취약점 분석·평가를 실시하면서 서버, 네트워크, DB, 보안장비 등 보유장비(△,△△△대)의 ▽.▽▽%(▲▲대)에 해당하는 장비에 대해서만 평가*하여 다수의 장비에 대한 보안취약점 대응이 어려우므로

* ☆☆☆그룹 자체적으로는 정보처리시스템에 대해 분기별 CIS벤치마크 수행과 매년 신용카드결제 정보의 안전한 처리와 관련하여 외부 보안인증(PCI-DSS)을 요청하여 수행 중

전자금융거래의 안전성과 신뢰성이 확보될 수 있도록 취약점 분석·평가 대상 장비를 확대하여 수행하시기 바람

다. 중요단말기 관리통제 미흡

회사는 「전자금융감독규정」 제12조에 따라 정보처리시스템에 직접 접속하는 중요단말기(◇◇대)를 지정하여 외부 반출, 인터넷 및 그룹웨어 접속 금지 등 강화된 보호대책을 적용하고 있으나

IT직원용과 전산센터 관리용 중요단말기를 사번과 비밀번호 인증만으로 내부통신망 접속이 가능하도록 운영하고 있고

내규 「□□□□□□□□ □□ □□□」에서 중요단말기의 물리적 보안통제와 관련하여 외부반출에 대한 사항*만 기술하고 있어 중요단말기의 지급 및 회수, 현황 파악 등에 대한 관리통제가 부족하므로

* 외부 반출 원천적 차단, 반출요청서를 통한 팀장의 결재 이후 제한적 반출 가능

중요단말기를 통한 내부통신망 접속 시 별도의 추가 인증을 적용하고, 중요단말기 관리에 필요한 세부사항을 내규화 하도록 개선하시기 바람

라. 프로그램 변경통제 미흡

내규 「◆◆◆◆◆◆ ◆◆◆◆ ◆◆◆」에 따라 프로그램 변경은 ☆☆☆☆ 및 ◎◎◎◎◎◎◎ 등을 통해서 요구사항 접수, 작업계획 수립, 설계 및 개발(개발자 테스트), 사용자 테스트를 거쳐 이루어지고 있는데

사용자가 임의로 테스트 시나리오 유형*을 선택할 수 있어 '목표 요구사항의 달성' 등과 같은 공통적이고 일반적 사항만 ◎◎◎◎에 사용자 테스트 결과로 입력하고 있고 개발유형 중 배치 프로그램은 '테스트 시나리오 및 결과서' 작성 대상으로 지정하지 않아 ◎◎◎◎◎◎◎에 개발자 테스트 결과를 등록하지 않는 등 테스트가 충실히 이루어지지 않을 우려가 있으므로

* 공통유형 및 개발유형(온라인/배치)에 따라 분류

사용자 테스트 시나리오는 개발유형에 따라 사전에 지정하고, 배치 프로그램에 대해서도 '테스트 시나리오 및 결과서'를 필수 작성 대상으로 지정하여 프로그램 변경에 대한 테스트가 충실히 이루어질 수 있도록 프로그램 변경통제 절차를 개선하시기 바람

마. 일괄작업 오류에 대한 통제 미흡

내규 「☆☆☆☆☆☆ ☆☆☆☆ ☆☆☆」 및 「◎◎◎◎◎ ◎◎◎ ◎◎ ◎◎◎」에 따라 ◇◇◇◇을 통해 일괄작업 요청을 받아 배치 스케줄러를 이용하여 신규, 변경, 실행 등의 작업을 처리하고 있으나

일괄작업 수행과정에서 오류가 발생하였을 경우 처리절차에 대한 내부규정 등이 마련되어 있지 않아 오류 발생 원인 및 대책 등의 세부 내용과 책임자의 확인 여부*를 기록·관리하고 있지 않으며

* 일괄작업 오류 발생 시 책임자 등에게 문자(SMS)만 발송

오류 발생으로 단순히 재실행이 필요한 경우 IT개발부서 담당자가 오퍼레이터에게

유선 등으로만 요청하고 별도의 요청기록은 남기지 않는 등 일괄작업 오류 처리와 관련된 관리 및 통제가 미흡하므로

일괄작업 수행 시 오류 처리를 위한 세부적인 절차를 마련하여 내부규정 등에 반영하고 철저히 이행하시기 바람